УДК 341.01
DOI https://doi.org/10.32782/2524-0374/2022-8/132

НОРМОТВОРЧА ДІЯЛЬНІСТЬ ООН ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ВОЄННІЙ СФЕРІ

UN NORMATIVE ACTIVITIES REGARDING ENSURING INFORMATION SECURITY IN THE MILITARY SPHERE

Сємко М.О., ст. викладач кафедри права
Національний технічний університет «Харківський політехнічний інститут»

Стаття присвячена аналізу діяльності ООН щодо забезпечення інформаційної безпеки у воєнній сфері. Встановлено, що міжнародна інформаційна безпека посідає провідне місце в системі міжнародних інформаційних відносин. У дослідженні під міжнародною інформаційною безпекою розуміється стан захищеності інформаційного середовища суспільства шляхом застосування сукупності економічних, політичних, юридичних заходів. Аналізом резолюцій ООН встановлено, що інформаційна безпека складається з трьох основних складових: протидія кіберзлочинності, протидія тероризму і забезпечення безпеки у воєнній сфері. Зроблено акцент на тому, що в резолюціях ООН більше уваги приділяється протидії кіберзлочинності та тероризму. Відповідно, міжнародна інформаційна безпека у воєнній сфері приділено набагато менше уваги.

У ході дослідження встановлено, що ООН було прийнято 25 резолюцій, які стосуються досягнень у сфері інформатизації і телекомунікації у контексті міжнародної безпеки. Питання воєнної безпеки у сфері ІКТ набуло актуального значення лише з 1998 року. При цьому у резолюціях ООН розгляд питання воєнної безпеки у сфері міжнародної інформаційної безпеки носив більше декларативний характер. Починаючи з 2015 року у резолюціях ООН акцентується увага на можливості використання інформаційно-комунікаційних технологій під час міжнародних конфліктів. У 2018 році резолюція ГА ООН A/73/27 від 19.11.2018 року закріплює звід з 13 правил відповідальної поведінки держав у сфері інформатизації і телекомунікації. У 2021 році на підставі Доповіді Робочої групи відкритого складу по питанням безпеки у сфері використання ІКТ та самих ІКТ 2021-2025 років чітко визначається необхідність застосування норм, принципів та звичаїв міжнародного права у сфері забезпечення міжнародної інформаційної безпеки. Підкреслюється необхідність формування нових норм, що регулюють міжнародну інформаційну безпеку у тому числі у воєнній сфері.

Ключові слова: міжнародна інформаційна безпека, міжнародна інформаційна безпека у воєнній сфері, загрози міжнародній інформаційній безпеці, нормотворча діяльність ООН.

The article is devoted to the analysis of UN activities in the field of information security in the military sphere. It has been established that international information security occupies a leading place in the system of international information relations. The study understands the state of protection of the information environment of society by means of the application of a combination of economic, political, and legal measures. An analysis of UN resolutions found that information security consists of three main components: The fight against cybercrime, the fight against terrorism, and the provision of security in the military sphere. Emphasis was placed on the fact that the UN resolutions pay more attention to the fight against cybercrime and terrorism. Accordingly, international information security in the military sphere has been given much less attention.

The study found that the United Nations had adopted 25 resolutions dealing with advances in information and telecommunications in international security. The issue of military security in the ICT sphere has become topical only since 1998. At the same time, UN resolutions considered the issue of military security in the sphere of international information security more declarative. Since 2015, UNO resolutions have focused on the possibility of using information and communication technologies in international conflicts. In 2018, the UN GA resolution A/73/27 of 19.11.2018 established states' 13 rules of responsible behaviour in the sphere of information and telecommunications. In January 2021, on the basis of the Draft substantive report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, the necessity of application of norms, principles, and customs of international law in the sphere of ensuring international information security is clearly defined. The need for new norms regulating international information security, including in the military sphere, is emphasized.

Key words: international information security, international information security in the military sphere, threats to international information security.

Постановка проблеми та актуальність дослідження. В широкому комплексі актуальних теоретично-прикладних питань, що досліджуються наукою міжнародного права, особливе місце посідає проблематика сучасних міжнародних інформаційних правовідносин. Міжнародні інформаційні зв'язки у вигляді відповідних суспільних відносин знаходять свій прояв та здійснюють вплив на світову науку, розробку сучасних технологій, доступність освіти, виробництво, екологічну та технологічну безпеку тощо. Однак, реалізація цих відносин неможлива без формування єдиного механізму міжнародно-правового регулювання, який базується на міждержавному співробітництві у інформаційній сфері і спрямований на захист прав та законних інтересів людини і держави.

Одним з важливих напрямків формування інформаційно-комунікаційного простору є міжнародна безпека, у тому числі у військовій сфері. Сьогодні на території сучасної Європи точиться наймасштабніший військовий конфлікт за останні 90 років, де інформаційно-комунікаційні технології (далі – ІКТ) виступають як фактором формування балансу сил, так і впливають на безпеку учасників міжнародних відносин. Це свідчить про важливість досягнень у сфері інформатизації та телекомунікації у контексті міжнародної безпеки у воєнній сфері. Відповідно, рівень міжнародно-правового регулювання ІКТ-сектору як важливого елемента міжнародної безпеки вимагає якісної наукової оцінки. При цьому нами акцентується увага саме на правотворчій діяльності ООН як організації, яка відповідно до ст. 1 свого Статуту покликана підтримувати міжнародний мир та безпеку і з цією метою здійснювати ефективні колективні заходи з метою попередження і усунення загрози миру та придушення актів агресії [1].

Стан наукової розробки. Питання регулювання інформаційних відносин та кібербезпеки нормами вітчизняного права досліджувались у працях І.В. Арістової, А.В. Войцеховського, М.Т. Гаврильціва, В.В. Галунька, А.І. Марущака, О.В. Марцеляка, В.В. Мицика, А.В. Пазюка, К.Ю. Примакова та інших. У свою чергу питання міжнародно-правового регулювання ІКТ як сфери міжнародної безпеки присутні у наукових розвідках таких науковців як Р. Арон, Дж. Кін, П. Келлер, Б. Крейг, Е. Меррей, Е. Пакард, М. Пестор, Ч. Різ тощо. Існує й низка вітчизняних праць, присвячених міжнародній інформаційній безпеці, зокрема, роботи А.О. Боднар, І.М. Забари, О.М. Фролової та інших. Водночас, досліджень, які стосуються досягнень у сфері інформатизації та телекомунікації

у контексті міжнародної безпеки у воєнній сфері недостатньо і вони не враховують сучасних реалій.

Мета статті полягає у з'ясуванні вкладу ООН у формування правового механізму забезпечення міжнародної інформаційної безпеки у воєнній сфері.

Завданнями роботи є: 1)формулювання та застосування норм, принципів та звичаїв міжнародного права у сфері забезпечення міжнародної інформаційної безпеки; 2) здійснення аналізу правових положень даного питання; 3) показати дієві колективні заходи з метою застереження і усунення загрози миру та приборкання актів агресії.

Виклад основного матеріалу. Світові інформаційні процеси набули широкого міжнародного значення ще наприкінці XIX століття через їх масове розповсюдження. А з появою у XX столітті глобальної телекомунікаційної мережі Інтернет, з'явилися нові питання, які потребують обов'язкового міжнародно-правового регулювання на засадах верховенства міжнародного права, правової компромісності, справедливості, міждержавної взаємодії, гуманізму, ефективності обігу міжнародної інформації, телекомунікативності тощо. В умовах війни, яка відбувається між Україною та Російською Федерацією не слід відкидати важливість впливу інформації на міжнародні політичні і безпекові процеси. Відповідно, на перший план у цьому протистоянні виходить міжнародна інформаційна безпека, предметом захисту якої виступає інформація, що має значення в умовах наявного міжнародного збройного конфлікту.

Аналізуючи поняття міжнародної інформаційної безпеки, слід відмітити, що у науковців не має єдиної позиції стосовно даного терміну, хоча у вітчизняних наукових дослідженнях саме термін "міжнародна інформаційна безпека" є найбільш розповсюдженим. При цьому зустрічаються назви "міжнародна кібербезпека" та "міжнародна інформаційна захищеність" [2]. У нашому дослідженні ми використовуємо більш розповсюджене поняття, а саме "міжнародна інформаційна безпека". При цьому ми підтримуємо наукову позицію П.Д. Біленчука, що міжнародна інформаційна безпека є стан захищеності інформаційного середовища суспільства та сукупність заходів різного характеру (економічного, політичного, юридичного), спрямованих на її підтримку [3, с. 64].

Особливого значення міжнародна інформаційна безпека набуває у воєнній сфері, у тому числі в умовах збройного конфлікту. Зрозуміло, що кожна держава, виступаючи учасником відносин, спрямованих на підтримку міжнародної безпеки формує власну стратегію розвитку інформаційної політики. Однак, виникає питання щодо безпечності такої політики для інших учасників міжнародних відносин та її так званої добропорядності. Саме данні, які з'являються у інформаційному просторі, впливають на стан подій на фронті, а також на ставлення світової спільноти до даних подій. Беручи в якості прикладу інформаційну війну, яка відбувається під час війни України та Росії, можна прийти до висновку про свідоме перекручення фактів і подій, створення фейкової інформації з боку ЗМІ РФ з метою формування негативного образу України як держави. Таким чином, слід погодитися з М. Дмитренко, що кібервійна, яка розгортається на фоні війни України та Росії, це "війна не за території, а за світогляд, думки і душі людей" [4, с. 240-241]. При цьому зазначимо, що думки і душі у даній війні не тільки українців, але й представників інших країн. Саме від останніх залежить надання військової та економічної допомоги Україні.

Окрім цього інформаційно-телекомунікаційні технології можуть бути використані у воєнній сфері з метою отримання інформації, яка стосується військової та оборонної сфер, зокрема, особистих даних про військовослужбовців, кількість та види озброєння, розташування мобільних та немобільних військових об'єктів, а також важливих для оборони об'єктів інфраструктури тощо. Зокрема, експерти Міністерства оборони РФ стверджують, що грамотний аналітик «вилучає все необхідне з того інформаційного поля, яке створюється звичайними людьми і розповсюджується у Мережі» [5]. І такі заяви з боку країни-агресора необхідно обов'язково враховувати як військовослужбовцям, так і пересічним громадянам, які висвітлюють діяльність Збройних Сил України через ті чи інші воєнні події.

Також за допомогою ІКТ можливе створення інформації, яка може вплинути на хід конфлікту або його початок. В якості прикладу впливу інформації на результати міжнародного конфлікту, його учасників та третіх сторін можна навести дипфейк промови Президента України В. Зеленського щодо капітуляції України 16 березня 2022 року.

Відповідно, міжнародна інформаційна безпека у воєнній сфері представляє собою систему міжнародних відносин, спрямованих на попередження кіберзагроз та захист від них міжнародної інфосфери до початку та в ході озброєного протистояння між державами.

Слід звернути увагу на те, що питання зв'язку між збройним конфліктом та інформаційними технологіями не нове. Зокрема, виокремлення військової складової у інформаційній безпеці на міжнародному та доктринальному рівні було підставою для жвавих дискусій як в ООН, так і між науковцями. Питання інформаційної війни як складової зовнішньої військової політики держави розглядалося і як застосування сили (що відповідно вимагає визнання її протиправного характеру та обмежень/заборони) і як звичний для мирного чи воєнного стану феномен, який не потребує додаткового міжнародно-правового регулювання [6, с. 84-86]. Ці дискусії стали підґрунтям для розвитку теорії інформаційної війни, що виникла у 90-ті роки XX століття і послугувала поштовхом для прийняття низки міжнародно-правових актів, спрямованих на правове регулювання відносин міжнародної інформаційної безпеки, у тому числі з урахуванням її військової складової.

Загалом станом на 2022 рік ООН було прийнято 25 резолюцій, які висвітлювали вплив інформаційно-комунікаційних технологій (далі – ІКТ) на сферу міжнародної безпеки. У грудні 1998 року Генеральною Асамблеєю ООН було прийнята резолюція 53/70 «Досягнення в сфері інформатизації і телекомунікації в контексті міжнародної безпеки», де зазначалося, що технології і засоби потенційно можуть бути використані в цілях, несумісних з задачами забезпечення міжнародної стабільності і безпеки та негативно впливати на безпеку держави. Були поставлені задачі щодо інформування Генерального секретаря щодо стану загальної інформаційної безпеки; необхідності визначення понять неправомірного використання інформаційних і телекомунікаційних систем і інформаційних ресурсів; доцільності розробки міжнародних принципів, спрямованих на зміцнення безпеки глобальних інформаційних та телекомунікаційних систем і інформаційних ресурсів [7]. Даний наратив знайшов своє відбиття у Резолюції ООН 54/49 «Досягнення в сфері інформатизації і телекомунікації в контексті міжнародної безпеки» від 1 грудня 1999 року, в якій вже конкретизувалося, що технології і засоби потенційно можуть бути використані у цілях несумісних з задачами забезпечення міжнародної стабільності і безпеки не тільки у цивільній, але й військовій сфері [8]. І хоча на підставі цих документів можна вважати, що ООН визнала факт існування проблеми інформаційної безпеки, прийняті резолюції неповністю відбивають ті проекти резолюцій, які надавалися державами і містили такі поняття як «інформаційна зброя» та «інформаційна війна» і схилялися більше до можливостей застосування інформаційних технологій у кримінальній сфері. Подібна тенденція щодо висвітлення питання міжнародної інформаційної безпеки у воєнній сфері простежуються і в резолюціях ООН № 55/28 від 20 листопада 2000 року, № 56/19 від 29 листопада 2001 року та інших. При цьому не дивлячись на тенденцію виявлення трьох

основних загроз міжнародній інформаційній безпеці – злочинність, тероризм і воєнна сфера, міжнародна спільнота продовжувала більше уваги приділяти двом першим загрозам. Зокрема, на рівні Ради Європи - Конвенція про кіберзлочинність від 22.11.2001 року та додатковий протокол до неї від 28.01.2003 року.

На питанні ж про міжнародну інформаційну безпеку у військовій сфері перший вагомий акцент робиться у 2015 році, коли у резолюції ГА ООН 70/455 [9] визначається, що досягнення науки і техніки можуть мати як цивільне так і військове застосування, що вимагає підтримки їх розвитку для виконання виключно у цивільній сфері та запропоновано виконувати принципи, передбачені Доповіддю Групи урядових експертів по досягненням у сфері інформатизації і телекомунікації у контексті міжнародної безпеки А/70/174 від 22.06.2015 року [10]. Зокрема, у Доповіді пропонуються заходи зміцнення довіри та розширення співробітництва на засадах міжнародних принципів гуманності, необхідності, пропорційності та індивідуалізації. Серед наявних загроз зазначається, що ряд держав займаються нарощуванням потенціалу у сфері ІКТ для військових цілей, що робить їх застосування у майбутніх конфліктах між державами більш вірогідним, зокрема, шляхом нападу на важливі об'єкти інфраструктури. Важливими висновками Групи стали позиції по відношенню застосування норм міжнародного права у використанні ІКТ державами, зокрема визнавалася юрисдикція держав на ІКТ-інфраструктурою, що знаходилася на їх територіях. При цьому процес використання ІКТ державами має здійснюватися на засадах таких принципів міжнародного права як державний суверенітет, суверенна рівність, вирішення засобів мирним шляхом, невтручання у внутрішніх справи інших держав, виконання обов'язків щодо поваги та захисту прав людини і основних свобод. Слід відмітити, що у наступних резолюціях ООН А/71/445 від 05.12.2016 року, А/73/27 від 19.11.2018 року зазначені пропозиції визначаються як провідні для всіх держав.

Також у резолюції ГА ООН А/73/27 від 19.11.2018 року сформований звід з 13 правил відповідальної поведінки держав у сфері інформатизації і телекомунікації: 1) держави повинні співпрацювати у розробці і здійсненні заходів щодо укріплення стабільності і безпеки у використанні ІКТ; 2) держави повинні виконувати свої міжнародні зобов'язання по відношенню міжнародно-протиправних діянь, які приписуються їм у відповідності до міжнародного права; 3) держави не повинні завідомо дозволяти використання своєї території для вчинення міжнародно-протиправних діянь з застосування ІКТ і використовувати посередників для вчинення таких діянь; 4) держави повинні розглядати питання щодо найкращих шляхів співробітництва з метою обміну інформацією, надання взаємодопомоги, переслідування осіб, винних у терористичному та злочинному використанні ІКТ; 5) дотримуватися положень резолюцій Ради по правам людини щодо захисту та забезпечення прав людини в Інтернеті та резолюцій ГА ООН про право на недоторканість особистого життя в епоху цифрових технологій; 6) держави не повинні підтримувати чи здійснювати діяльність, яка протирічить їх міжнародним зобов'язанням; 7) здійснювати належні міри щодо захисту своєї критичної інфраструктури від загроз у сфері ІКТ; 8) держави повинні задовольняти прохання про надання допомоги від інших держав у разі вчинення щодо низ злочинних дій у сфері ІКТ, у тому числі якщо такі дії здійснюються з їх території; 9) держави мають здійснювати заходи щодо забезпечення безпеки продуктів ІКТ; 10) попереджати розповсюдження злочинних програмних і технічних засобів у сфері ІКТ; 11) сприяти наданню інформації про вразливості у сфері ІКТ і ділитися відповідною інформацією; 12) не підтримувати діяльність, покликану нанести шкоду інформаційним системам іншої держави; 13) сприяти підвищенню ролі приватного сектора та громадянського суспільства в укріпленні безпеки системи ІКТ [11].

У 2019 році ГА ООН звертаючи увагу на те, що ряд держав займається нарощуванням потенціалу у сфері ІКТ для військових цілей, що робить їх використання вірогідними у майбутніх конфліктах та враховуючи власну роль у формуванні єдиного розуміння міжнародно-правового регулювання діяльності держав у сфер ІКТ створює на підставі Резолюції А/74/363 від 12.12.2019 року [12] Робочу групу ООН відкритого складу по досягненням у сфері інформатизації і телекомунікації у контексті міжнародної безпеки. Вона наряду з Групою урядових експертів визначена у якості незалежних механізмів ООН з підтримання міжнародного міру та безпеки у сфері використання інформаційно-комунікаційних технологій.

Підтримуючи необхідність діяльності Робочу групу ООН відкритого складу по досягненням у сфері інформатизації і телекомунікації у контексті міжнародної безпеки, ООН у резолюції A/RES/75/240 від 31.12.2020 року визначає необхідність формування нової Робочої групи відкритого складу по питанням безпеки у сфері використання ІКТ та самих ІКТ на 2021-2025 рік з метою напрацювання норм, правил і принципів відповідної поведінки держав з метою забезпечення безпеки у сфері використання ІКТ. Однак, знову ж таки згадана резолюція не наполягає на міжнародному регулюванні використання ІКТ, визначаючи, що добровільні та незобов'язуючі норми, правила та принципи поведінки держав у сфері ІКТ можуть знизити ризик порушення міжнародного миру, безпеки і стабільності [13]. Вкладені у цій зазначені резолюції положення знайшли своє продовження і у резолюції ГА ООН A/RES/76/19 від 6 грудня 2021 року. При цьому ГА ООН пропонує державам дотримуватися пропозицій, створених під час роботи Робочої групи відкритого складу по питанням безпеки у сфері використання ІКТ та самих ІКТ 2021-2025 років [14]. Зокрема, Проект предметної доповіді Робочої групи відкритого складу по досягненням у сфері інформатизації і телекомунікації у контексті міжнародної безпеки від 19 січня 2021 року містить наступні твердження щодо забезпечення інформаційної безпеки у воєнній сфері з метою формування відповідальної поведінки держав в сфері ІКТ. Зокрема: 1) необхідність застосування норм міжнародного права до використання ІКТ державами (загальних принципів, договорів та звичаїв) з його подальшим доопрацюванням; 2) застосування з метою зниження ризиків для цивільних осіб і цивільних об'єктів у ході збройних конфліктів міжнародного гуманітарного права з урахуванням недопущення застосування сили у будь-якій сфері, у тому числі ІКТ; 3) вказівка на те, що будь-яка діяльність у сфері ІКТ була розпочата з території конкретної держави чи об'єктів ІКТ-інфраструктури цієї держави може бути недостатньою для звинувачення цієї держави, відповідно обвинувачення повинні бути обґрунтованими; 4) необхідність розробки додаткових керівних вказівок у цій сфері; 5) одним із перспективних напрямків розробки заходів забезпечення інформаційної міжнародної безпеки можна вважати прийняття політичного зобов'язання; 6) необхідність чіткого визначення видів діяльності, пов'язаних з ІТК, які можуть бути оцінені державами як загроза силою та її застосування [15].

Висновок. Отже, аналіз резолюцій ГА ООН з 1998 по 2021 рік дає змогу прийти до висновків, що ООН не вбачає нагальної потреби у створенні системи конкретних міжнародних норм, які б створювали єдиний механізм забезпечення міжнародної інформаційної безпеки у військовій сфері та під час збройних конфліктів. Усвідомлюючи важливість даного питання, Організація перекладає відповідальність у цій сфері безпосередньо на держави у межах їх територіальної юрисдикції, хоча цілком зрозуміло, що ІКТ вже давно вийшли за межі конкретних

територій, а приватний сектор задіяний у створенні метавсесвіту. Таким чином, слід стверджувати про те, що існує необхідність створення єдиного міжнародного механізму забезпечення інформаційної міжнародної безпеки у всіх сферах. Однак, враховуючи негативний досвід залучення ІКТ під час війни України з РФ, міжнародна спільнота має звернути безпосередню увагу саме на інформаційну безпеку у воєнній сфері.

ЛІТЕРАТУРА

1. Статут Організації Об'єднаних Націй і Статут Міжнародного Суду ООН від 26.06.1945. URL: https://zakon.rada.gov.ua/laws/show/995_010#Text (дата звернення до ресурсу 01.07.2022 року)

2. Ісмайлов К.Ю. Поняття «кібезбезпека та «інформаційна безпека». Типологія безпеки. Міжнародна науково-практична конференція «Актуальні проблеми автоматизації та управління». Луцьк, 2016. С. 32-33.

3. Біленчук П.Д. Правові засади інформаційної безпеки України. Харків, 2018. 289 с.

4. Дмитренко М.А. Проблемні питання інформаційної безпеки України. Міжнародні відносини. Серія Політичні науки. 2017. № 17. С. 236–243.

5. Эксперт рассказал, как военные получают данные о военных объектах ВСУ. URL: https://www.mk.ru/politics/2022/04/19/ekspert-rasskazal-kak-voennye-poluchayut-dannye-o-voennykh-obektakh-vsu.html (дата звернення до ресурсу 03.07.2022 року)

6. Забара І.М. Правове регулювання військової складової міжнародної інформаційної безпеки. Актуальні проблеми міжнародних відносин. 2013. Випуск 117 (частина ІІ). С. 84-91.

7. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности. Резолюция, принятая Генеральной Ассамблеей ООН A/RES/53/70 4 декабря 1998 года. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement (дата звернення до ресурсу 29.06.2022 року).

8. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности. Резолюция, принятая Генеральной Ассамблеей ООН A/RES/54/49 1 декабря 1999 года. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/777/15/PDF/N9977715.pdf?OpenElement (дата звернення до ресурсу 29.06.2022 року).

9. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности. Резолюция, принятая Генеральной Ассамблеей ООН A/70/455 от 18 ноября 2015 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/374/17/PDF/N1537417.pdf?OpenElement (дата звернення до ресурсу 29.06.2022 року).

10. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности A/70/174 от 22.06.2015 года. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement (дата звернення до ресурсу 01.07.2022 року).

11. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности. Резолюция, принятая Генеральной Ассамблеей ООН A/RES/73/27 от 11 декабря 2018 года. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/07/PDF/N1841807.pdf?OpenElement (дата звернення до ресурсу 29.06.2022 року)

12. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности. Резолюция, принятая Генеральной Ассамблеей ООН A/74/363 от 12 декабря 2019 года URL: https://documents-dds-ny.un.org/doc/UNDOC/LTD/N19/344/59/PDF/N1934459.pdf?OpenElement (дата звернення до ресурсу 29.06.2022 року)

13. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности. Резолюция, принятая Генеральной Ассамблеей ООН A/RES/75/240 от 31 декабря 2020 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/28/PDF/N2100028.pdf?OpenElement (дата звернення до ресурсу 29.06.2022 року)

14. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности и поощрение ответственного поведения государств в сфере использования информационно-коммуникационных технологий. Резолюция, принятая Генеральной Ассамблеей ООН A/RES/76/19 от 6 декабря 2021 года. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/377/51/PDF/N2137751.pdf?OpenElement (дата звернення до ресурсу 29.06.2022 року).

15. Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Проект предметного доклада (первоначальный проект) от 19 января 2021 года. URL: https://documents-dds-ny.un.org/doc/UNDOC/LTD/N20/378/96/PDF/N2037896.pdf?OpenElement (дата звернення до ресурсу 02.07.2022 року).